SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS

OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, AND 30

1. REQUISITION NUMBER	PAGE 1 OF 86
M2638120SUH2FUL	

2. CONTRACT NO.	3. AWARD/EFFECTIVE DATE	4. ORDER NUMBER	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
W52P1J18DA023	16-Jun-2020	M6786120F0009	M6786120R0001	

7. FOR SOLICITATION INFORMATION CALL:	a. NAME	b. TELEPHONE NUMBER (No Collect Calls)	8. OFFER DUE DATE/LOCAL TIME
	(b)(6)	(504) 697-8348	

9. ISSUED BY CODE M67861

MARFORRES REGIONAL CONTRACTING OFFICE
MFR RCO
2000 OPELOUSAS AVE
NEW ORLEANS LA 70114

TEL: 504-697-8357
FAX:

10. THIS ACQUISITION IS

- [ ] UNRESTRICTED OR [X] SET ASIDE: 100 % FOR:
- [X] SMALL BUSINESS
- [ ] WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM
- [ ] HUBZONE SMALL BUSINESS
- [ ] EDWOSB
- [ ] SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS
- [ ] 8(A)

NAICS: 541519

SIZE STANDARD: $30,000,000

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED

- [ ] SEE SCHEDULE

12. DISCOUNT TERMS
NET 30 DAYS

- [ ] 13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)

13b. RATING

14. METHOD OF SOLICITATION

- [ ] RFQ
- [ ] IFB
- [X] RFP

15. DELIVER TO CODE M26381

G-6 MARFORRES
(b)(6)
2000 OPELOUSAS AVENUE
NEW ORLEANS LA 70114

16. ADMINISTERED BY CODE

SEE ITEM 9

17a. CONTRACTOR/ OFFEROR CODE 1HXK0 FACILITY CODE

AGILE DEFENSE, INC.
(b)(6)
11600 SUNRISE VALLEY DR STE 440
RESTON VA 20191-1425

TELEPHONE NO. 571-748-4455

- [ ] 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER

18a. PAYMENT WILL BE MADE BY CODE M67443

DFAS COLUMBUS
ATTN: VENDOR PAY
3990 EAST BROAD STREET, BUILDING 21
COLUMBUS OH 43213

18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a. UNLESS BLOCK BELOW IS CHECKED [ ] SEE ADDENDUM

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/ SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	SEE SCHEDULE				

25. ACCOUNTING AND APPROPRIATION DATA

See Schedule

26. TOTAL AWARD AMOUNT (For Govt. Use Only)

- [ ] 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1. 52.212-4. FAR 52.212-3. 52.212-5 ARE ATTACHED. ADDENDA [ ] ARE [ ] ARE NOT ATTACHED
- [ ] 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA [ ] ARE [ ] ARE NOT ATTACHED

- [X] 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN 1 COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED.

REF: 313086

- [ ] 29. AWARD OF CONTRACT: REF. OFFER DATED 09-Apr-2020 . YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS: SEE SCHEDULE

30a. SIGNATURE OF OFFEROR/CONTRACTOR

31a. UNITED STATES OF AMERICA (SIGNATURE OF CONTRACTING OFFICER)

(b)(6)

30b. NAME AND TITLE OF SIGNER (TYPE OR PRINT)	30c. DATE SIGNED	31b. NAME OF CONTRACTING OFFICER (TYPE OR PRINT)	31c. DATE SIGNED
		(b)(6) / OCS TEL: 504-697-9027 EMAIL: (b)(6) usmc.mil	16-Jun-2020

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION IS NOT USABLE

STANDARD FORM 1449 (REV. 2/2012)
Prescribed by GSA – FAR (48 CFR) 53.212

In addition to the maintenance and expansion of the existing Power BI dashboard products, IMKM expects to develop an additional 100+ dashboards and reports over the next year for every MSC, Regiment, Squadron, Group, and Battalion level commands as well as Primary and Special staff sections for MFR, at a minimum, in order to meet the intent of CMFR in using BI products to enhance decision making and reporting throughout the force. Features of this expansion include:

- Tailored access based on unit level permissions, PII, and FOUO, i.e. security trimmed
- Automatic Interfaces with enterprise and local authoritative data sources
- Integration with MFR SharePoint
- A Common, integration of data across the Force

The following is just the current backlog for new dashboards for MSCs and their commands:

4TH MARDIV: 30 each
4TH MAW: 28 each
4TH MLG: 12 each
FHG: 13 each

Due to the overall increase in demand for IMKM products and support as well as the shifting landscape of technologies, IMKM requires an additional five (5) contractor personnel in order to meet customer requirements and mission assurance as follows:

- Task area 5.2 Database Management and Maintenance – one (1) additional SQL Database Administrator/Engineer required;

- Task area 5.5 Software Engineering – two (2) additional personnel required: one (1) Senior Software Engineer and one (1) Junior Software Engineer.

- Task Area 5.6 SharePoint Development and Administration – two (2) additional personnel required: two (2) SharePoint Developer Mid personnel.

The personnel identified above will directly support IMKM and MARFORRES in the task areas detailed below which include custom application and Power BI report development as well as custom SharePoint and SQL solutions.

For the purposes of incorporating the surge into the PWS, blue text herein indicates where tasks to support the surge overlap existing tasks within the task order. Red text reflects either additional tasks, revisions, or the incorporation of additional granularity to the existing PWS. PowerBI is not specifically mentioned in the original PWS; this was an oversight on the part of the Government and is corrected via this modification as Functional Area 5.6, SharePoint Development and Administration, is utilizing PowerBI.

The following have been modified:

PERFORMANCE WORK STATEMENT

MARINE FORCES RESERVE PROFESSIONAL INFORMATION TECHNOLOGY SYSTEMS ARCHITECTURE AND APPLICATION SERVICES

(PWS)

1.0 PURPOSE

The purpose of this Performance Work Statement (PWS) is to obtain contractor support for a variety of professional information technology (IT) systems architecture and application services in support of the Marine Forces Reserve (MARFORRES) mission. The services to be provided include, but are not limited to; operations & maintenance, infrastructure support, application development and maintenance, and program support management.

2.0 BACKGROUND

The Marine Forces Reserve is a three-star General level command responsible for training and equipping approximately 160 geographically dispersed Marine Reserve units across the United States to augment and reinforce active Marine forces in time of war, national emergency or contingency operations, provide personnel and operational tempo relief for the active forces in peacetime, and provide service to the community. The geographical disbursement of Marine Forces Reserve units requires significant investment in Command and Control IT solutions. The IT services identified in this PWS are critical to maintaining, sustaining, and evolving the Command and Control platforms for the Commander, Marine Forces Reserve.

3.0 SCOPE AND OBJECTIVES

The scope of this Professional IT System Architecture and Application Services task order is to provide the necessary level of professional and technical support to facilitate the shared objectives of the MARFORRES staff and stakeholders to meet the Command and Control mission of the force.

The IT Operations Infrastructure Sustainment Support consists of the following major task areas that will be introduced further in the requirements section of this PWS:

- Network Administration
- Database Management and Maintenance
- Server Administration
- Telecommunication Maintenance
- Software Engineering
- SharePoint Development and Administration
- Program Management

4.0 GENERAL REQUIREMENTS

4.1 Applicable Directives

4.1. Applicable Directives.
• DoD 8570.01M (Incorporating Change 3, January 24, 2012)
• Marine Forces Reserve Knowledge Management Strategy
• Marine Forces Reserve SharePoint Governance
• Marine Forces Reserve Cybersecurity
• DoD 8570.01M (Incorporating Change 3, January 24, 2012)
• UFC 4-030-01 Sustainable development
• Energy Independence and Security Act of 2007 (EISA)
• Executive Order 13423 (Signed by the President on January 24, 2007)
• Executive Order 13514 (Signed by the President on October 5, 2009)
o MCO 5000 Series
o MCO P5090.2A

o SECNAVINST 5000.2D
• DoD Financial Management Regulations 7000.14-R
• Marine Corps Order P7300.21B
• DoD 5400.11 Department of Defense Privacy Program
• DoD IT Portfolio Repository User Guide ver 1.0 June 2011
• DoD 8570.01M (Change 3, January 24, 2012)
• DoD Financial Management Regulations 7000.14-R
• Marine Corps Order P7300.21B
• DoD 5400.11 Department of Defense Privacy Program
• DoD 8570.01M (Change 3 January 24, 2012)
• ALNAVs
• NAVADMINs
• ALMARs
• MARADMINs
• DoDD 2000.12, DoD Antiterrorism Program
• DoDI 2000.16, DoD Antiterrorism Standards
• DoD 2000.12-H, DoD Antiterrorism Handbook
• DoDI 3001.02 Personnel Accountability in Conjunction with Natural or Manmade Disasters
• DoD 3020.45-M, Volume 3, "Defense Critical Infrastructure Program (DCIP) Security Classification Manual (SCM)"
• DoDI 3020.52, "DoD Installation CBRNE Preparedness Standards"
• DoDD Minimum Antiterrorism Standards for Buildings
• DoD Minimum Antiterrorism Standoff Distances for Buildings
• DoDD 4500, 54-G, DoD Foreign Clearance Guide
• DoDD 6490.2 Joint Medical Surveillance
• DoDI 6055.17 Installation Emergency Management (IEM) Program
• DoDI 6500.17 DoD Installation Emergency Management Program
• DHS, National Response Framework (NRF)
• Unified Facilities Criteria (UFC) 4-010-01, DoD Minimum Antiterrorism Standards for Buildings
• UFC 4-010-02, DoD Minimum Antiterrorism Standoff Distance for buildings
• UFC 4-021-01, Design and O&M:Mass Notification Facilities
• NAVMC 3500.103, "Marine Corps Antiterrorism Manual"
• MCO 3305X02.1E, "Marine Corps Antiterrorism Program"
• MCO 3501.36A, "Marine Corps Critical Infrastructure Program"
• MCO 3504.2, "Marine Corps Lessons Learned Program and The Marine Corps Center for Lessons Learned"
• MCO P5530.14A "Marine Corps Physical Security Program"
• NAVMC 3500.103, "Marine Corps Antiterrorism Manual"
• MCO 3440.8 "Installation Chemical, Biological, Radiological, Nuclear and High-Yield Explosive (CBRNE)Protection Program"
• MCO 3440.9 "Installation Emergency Management"
• FORO 3440.1H Continuity of Operations (COOP)Program Management
• FORO 3070 (DRAFT) Operations Security (OPSEC)
• FORO P5510.1B Standard Operating Procedures for the Information and Personnel Security Program
• FORO 6200 (DRAFT) Pandemic Influenza (PI)
• Marine Forces Reserve Standard Operating Procedures (SOP)
• Marine Forces Reserve MCEITS Share Point Portal https://eis.usmc.mil/sites/MARFORRESg3ma
• Defense Threat Reduction Agency Security Classification Guide
• USPACOM Instruction 0614.1 "Theater Travel Requirements in U.S. Pacific Command (USPACOM)
• MCCRAM 1009.1K – Foreign Travel Policy
• APACs
• DISA PPSM Security Classification Guide - Jan 2006

• DISA DoD Ports, Protocols, and Services User Guide - Sep 2012
• DOD CIO Memorandum - Guidance for Cybersecurity Workforce Certification
Compliance Process - Feb 2012
• DOD O-8530.2 - Support to Computer Network Defense (CND) - Mar 2001
• DODD 3020.26 - Department of Defense Continuity Programs - Jan 2009
• DODI 8550.01 - DoD Internet Services and Internet-Based Capabilities – Sep 2012
• DODI 8500.01 - Cybersecurity - Mar 2014
• DODI 8510.01 - Risk Management Framework (RMF) for DoD Information Technology (IT) - Mar 2014
• DODI 8551.01 - Ports, Protocols, and Services Management (PPSM) - May 2014
• DON SECNAV Ins 5230.15 - Information Management IT Policy for Fielding of COTS Software - Apr 2009
• DON SECNAV Ins 5239.20 - DON Cybersecurity and IA Workforce Management – Jun 2010
• SECNAV M-5239.2 Cyberspace Info Tech and Cybersecurity Workforce MGMT and Qualification- June 2016
• MARFORRES Cyber Security Directive Ver2.1 dtd 2013-05-07
• MARFORES FORCE ORDER 2000-1.4
• MC ECSD 020 - Information Assurance Vulnerability Management Program (IAVM) -Dec 2013
• MC ECSD 021 - Ports Protocols and Services Management Version 1 - May 2012
• MC ECSM 018 - Marine Corps Assessment and Authorization Process Version 4.0
• MC Order 5239.2B - Marine Corps Cybersecurity - Nov 2015
• MCIP 3-40.02 - Marine Corps Cyberspace Operations - Oct 2014
• MCWP 3-40.4 - MAGTF Information Operations - Jul 2003
• DoD Directives (DoDD) 8500.01p, "Information Assurance (IA), dated 24 October 2002. Certified current 23 April 2007
• DoD Instruction (DoDI) 8100.3, DoD Voice Networks, dated January 16, 2004
• DoDI 8500.2, "Information Assurance (IA) Implementation," dated 6 February 2003
• DoDI 8510.01, "DoD Information Assurance Certification and Accreditation Process, "dated 28 November 2007.
• DoDI 8551.1, Ports, Protocols, and Services Management (PPSM)." Dated 13 August 2004
• DoDI 8560.01, Communication Security, COMSEC) Monitoring and Information Assurance (IA) Readiness Testing, dated 9 October, 2007
• DoD 52220.22-M, National Industrial Security Program, dated 28 February, 2006
• Committee on national Security Systems Instruction (CNSSI) No. 40009, "National Information Assurance (IA) Glossary," as revised June 2006.
• Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6215.01C, Policy for Department of Defense (DOD) voice Networks with Real Time Services (RTS), dated 9 November 2007.
• CJCSI 6211.02C, Defense Information System Network (DISN): Policy and Responsibilities, dated 9 July 2008
• National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18, Guide for Developing Security Plans for Federal Information Systems, revision 1
• Defense Information Systems Agency (DISA) Field Security Operations (FSO) Security technical Implementation Guides (STIGs): http://iase/disa.mil/stigs/
• DISA FSO Security Checklists: http://iase.dis.mil/stigs/checklist
• National Information Assurance Partnership (NIAP) WEB SITE: http://WWW.NIAPCCEVS.ORG/
• Unified Capabilities Certification Office (UCCO) Approved Products List (APL) removal List: http://www.disa.mil/uccco/apl_removal.html.
• DIS, Joint Interoperability Test Command (JITC) DoD Unified Capabilities (UC) Requirement, Process and Test Documents: http://jitc.fhu.disa.mil/apl/dsn.html

4.2 Working on a Government Installation

4.2.1 Contractor employees must be clearly identifiable while on Government property by wearing Government issued badges. These badges shall be worn at all times and presented for examination upon request from the Contracting Officer, Contracting Officer Representative (COR), Quality Assurance (QA) Personnel, Military Police, or any other Government Official with a need to see the badge.

4.2.2 The Contractor and its employees shall be subject to all traffic, security, and registration regulations for personnel and vehicles. Copies of current regulations may be obtained from the Contracting Officer.

4.2.3 All Contractor personnel attending meetings, answering Government telephones, receiving or responding to electronic messages and correspondence related to this task order, working on site or where their Contractor status is not known to third parties, must identify themselves as Contractors, to include wearing ID badges, which identify them as Contractor personnel. Contractor personnel shall also ensure that when logged onto Government equipment that their profile shows them as Contractor personnel. Unless otherwise directed by the COR, all documents produced or revised by Contractors or developed through Contractor participation must be marked as "Contractor generated documents" or otherwise identified in a manner that discloses the Contractor's participation.

4.2.4 Contractor-occupied facilities (on Government installations) such as offices, separate rooms, or cubicles must be clearly identified with Contractor supplied signs, name plates or other identification, showing that these are work areas for Contractor personnel.

4.3. Security Requirements.

Security requirements applicable to this task order are described in the Department of Defense Contract Security Classification Specification DD Form 254 (Attachment # 1).

All personnel performing tasks under this task order must be eligible for, and obtain, a DoD Common Access Card (CAC) and associated DoD Public Key Infrastructure (PKI) certificates for identity verification and encryption of transmitted correspondence.

Contractor personnel may require access to facilities after hours. Consequently, Contractor personnel shall follow procedures established at each site for ensuring the security of the building, equipment, materials and personnel who are working in and around facilities. During duty hours, Contractor personnel shall keep doors to the outside of facilities secured except the ones used by customers. When securing facilities at the end of the duty day, Contractor personnel shall follow established procedures.

- All personnel working under this task order must have an active DoD Secret level security clearance. Interim security clearances are acceptable for personnel at the start of performance under this task order; the Contractor must maintain an Interim clearance until the Active Secret Level clearance is approved.

- The contractor must have an active DoD Secret level facility clearance or, an Interim facility security clearance prior to task order award; the Contractor must maintain an Interim facility clearance until the Active Secret Level facility clearance is approved.

- Personal security clearance requests are processed by the Defense Industrial Security Clearance Office (DISCO), which is located in Columbus, OH. Recent changes require the contractor to establish Security clearances. Employees assigned to this task will require IT-II

designation and will require a favorably adjudicated DoD Secret or National Agency Check with Local Agency Check/ Access National Agency Check with Inquiries (NACLC/ANACI) which will be updated every ten years by a NACLC.

4.4 HISTORICAL STAFFING

4.4.1 Historical Task Area Staffing

For reference purposes, the below table represents historical Full Time Equivalent (FTE) staffing for each task area. Although the Government is providing this as a reference, contractors are encouraged to optimize a staffing approach solution in their proposals to meet the tasks outlined in this PWS.

NOTE: There is not a currently approved solution at MARFORRES for VPN access to classified material for a telework use. Support of the SharePoint Development Administration functional area is the only task area authorized for tele-work.

TASK AREA	Number of FTE's
Network Administration	3
Database Management and Maintenance	2
Server Administration	3
Telecommunications Maintenance	1
Software Engineering	5
SharePoint Development and Administration	5
IT Ops & Maintenance Program Management	1

4.4.2 Quality Control Plan (QPC)

The government shall evaluate the Contractor's performance under this contract in accordance with the Contractors Quality Control Plan (QCP) and the Governments Quality Assurance Surveillance Plan (QASP). The Contractor shall submit a Quality Control Plan (QCP) that addresses the following:

- Contractor's plan to ensure timely delivery of deliverables, ensure quality of deliverables and how quality deficiencies in deliverables will be mitigated, standards of acceptance, and interactions between the Contractor and the COR(s) to ensure effective communication, management of tasks and quality assurance.
- Demonstrate the Contractor approach to meeting the quality metrics.
- Discuss the Contractor methodology and staffing responsibilities for identifying deficiencies in the quality of services performed before the level of performance is unacceptable.

4.4.3 Quality Assurance Surveillance Plan (QASP)

Quality Assurance (Attachment 2): The QASP is a Government developed and applied document used to make sure systematic quality assurance methods are used in the administration of the Performance Based Service Contract (PBSC) standards included in this Performance Work Statement (PWS) and contract. The intent is to ensure that the Contractor performs in accordance

with the performance metrics and the Government receives the quality of services called for in the contract. The QASP details how the performance standards identified in the PWS will be measured, who will perform the measurement, the frequency of surveillance, and the acceptable defect rate(s). The QASP may be updated from time to time by the government.

4.5 KEY PERSONNEL

4.5.1 The Contractor shall provide the required number of "key personnel" for each respective performance task area. Each performance task will have specific qualifications, which can be found in each task area's section of this PWS.

4.5.2 Key Personnel is defined as certain skilled, experienced, professional and/or technical personnel who is or are specifically and uniquely essential for successful contractor accomplishment of the work to be performed under this task order. These are defined as "Key Personnel" and are those persons whose resumes were submitted for evaluation of the proposal. The contractor agrees that such personnel shall not be removed from the task order work or replaced without compliance with section 5.2 Substitution of Key Personnel of this Performance Work Statement.

TASK AREA	Number of Key Personnel	Labor Category
Network Administration	1	SENIOR
Database Management and Maintenance	1	INTERMEDIATE
Server Administration	1	SENIOR
Telecommunications Maintenance	1	SENIOR
Software Engineering	2	SENIOR
SharePoint Development and Administration	1	INTERMEDIATE
IT Ops & Maintenance Program Management	1	SENIOR

The labor category "Senior" is defined as an employee who has over 10 years of experience in their respective fields or comparable fields and possesses a BA/BS or MA/MS degree. A senior employee typically works on high-visibility or mission critical aspects of a given program and perform all functional duties independently. A senior employee may oversee the efforts of less senior staff and /or be responsible for the efforts of all staff assigned to a specific job.

An "Intermediate" employee has more than 5 years of experience and possesses a BA/BS or MA/MS degree. An Intermediate employee typically performs all functional duties independently.

"Associate," remains as defined in the base IDIQ under the Army's CHESS ITES-3S program with no deviation.

4.6 SUBSTITUTION OF KEY PERSONNEL

4.6.1 Guidance on Substitutions. During the first ninety (90) days of the task order performance period no key personnel substitutions by the Contractor will be made unless substitutions are necessitated by an individual's sudden illness, death, termination of employment or non-acceptance of an offer of employment. In any of these events, the Contractor shall promptly notify the Contracting Officer and provide the information required by Section 5.2.3 below.

After the initial ninety (90) day period, all proposed substitutions must be submitted to the Contracting Officer and provide information required by Section 5.2.3 below, in writing, at least 10 days in advance of the proposed substitutions, when possible.

If one or more of the key personnel for whatever reason becomes, or is expected to become, unavailable for work under this task order for a continuous period exceeding thirty (30) work days, or is expected to devote substantially less effort to the work than indicated in the proposal or initially anticipated, the contractor shall immediately notify the Contracting Officer and shall, subject to the concurrence of the Contracting Officer or his authorized representative, promptly replace such personnel with personnel of at least substantially equal ability and qualifications.

4.6.2 Request for Substitution. All requests for substitutions must be in writing and provide a detailed explanation of the circumstances necessitating the proposed substitution, a resume for the proposed substitute, and any other information requested by the Contracting Officer. All proposed substitutes must have qualifications equal to or higher than the qualifications stated in the PWS. They must contain a complete resume for the proposed substitute, and any other information requested by the Contracting Officer or needed by him to approve or disapprove the proposed substitution. The Contracting Officer or his/her authorized representative will evaluate such requests and promptly notify the Contractor of his/her approval or disapproval thereof.

If the Contracting Officer determines that suitable and timely replacement of key personnel who have been reassigned, terminated or have otherwise become unavailable for the task order work is not reasonably forthcoming or that the resultant reduction of productive effort would be so substantial as to impair the successful completion of the task order or the services ordered, the task order may be terminated by the Contracting Officer for default or for the convenience of the Government, as appropriate, or, at the discretion of the Contracting Officer if he/she finds the contractor at fault for the condition, the task order price may be equitably adjusted downward to compensate the Government for any resultant delay, loss, or damage.

5.0 PERFORMANCE TASKS

The Contractor shall arrange a kick-off meeting within ten (10) business days after task order award. The meeting shall be held at the Marine Forces Reserve Regional Contracting Office (MFR-RCO). The Contractor shall contact the Contracting Officer and COR to arrange the specific date and time of the meeting. All available key personnel are required to attend the kick-off meeting.

Available' is defined as, as any key personnel hired by the contractor in direct support of the resulting task order. In person attendance of all available key personnel team members is desired, however, attendance via phone conference is also acceptable

The Contractor shall be contractually obligated to perform every requirement in this PWS. Not every performance requirement has a related performance standard or assessment measure expressed in this document. In such cases, the performance measure is inherent in the requirement.

Each task area outlined below will follow the below format:

- General overview
- Minimum certification requirements
- Performance tasks
- Deliverables

5.1 Network Administration

General Overview

The contractor shall ensure full network mission capability by providing Tier III senior level technical support to MARFORRES WAN/BAN/LAN serving its Headquarters at Marine Corps Support Facility New Orleans and approximately 160 remote sites. Below outlines the current operating environment for this task area:

- Consists of approximately 1,000 Network devices at 160 sites and two data centers including both classified and unclassified networks.
- Approximately 8,000 end user devices on the unclassified network and 1,000 end user devices on the classified network.
- There are typically around 10,000 active users but, MARFORRES can support approximately 30,000 possible users.
- Two Data Centers built on Cisco Nexus and Unified Computing System (UCS) technology.
- Marine Forces Reserve Cyber range node (a network lab test and development environment).
- Current Network Devices and tools include but are not limited to: Cisco Catalyst 6500; Cisco Catalyst 4500; Cisco Catalyst 9300; Cisco Catalyst 3850; Cisco Catalyst 3750; Cisco Catalyst 3560; Cisco Nexus Devices; Cisco ASR 1002; Cisco ASR 1006; Cisco 2900 series routers; Cisco 3900 series routers; Cisco 4000 series routers; Cisco ISE with TACACS/Network Device Management Integration to include support for multifactor authentication; Aruba and HP wireless network infrastructure; Forescout CounterAct; High Assurance Internet Protocol Encryptors; Solarwinds Kiwi Tool suite; Riverbed Steelhead; GEM-X encryptor management system.
- Cisco Enhanced Interior Gateway Routing Protocol (EIGRP) and Border Gateway Protocol (BGP).
- High Availability Internet Protocol Encryptors for Classified environments including related Key Material.
- Network Common Operation Picture and Network Device Management is currently provided by: HP Network Node Manager I and HP Network Automation.
- Network Access control (NAC/802.1x) and Network Device Management is currently provided by: Cisco Identity Services Engine (ISE); TACACS+ via Device Administration License in Cisco ISE.
- Network Access control (NAC/802.1x) is moving to: Forescout Counteract.
- Backup Network Configuration automation is provided by: Kiwi Cattools.
- Log management is currently provided by Kiwi Syslog, moving to enterprise McAfee SIEM solution.
- WAN accelerators are currently Riverbed models.
- DHCP Servers are running on Windows servers.
- Redseal, DISA Assured Compliance Assessment Solution (ACAS) and STIG Checklists are primary used to ensure compliance with Cybersecurity directives.
- Typically 6-10 Design projects/Change Request drafts in progress at a time within Network Administration Section.
- Support escalated or high priority outage tickets as required for networks at 160 consisting of around 1,000 network devices. Majority of tickets are handled at lower tiers.

Minimum Certification Requirements

The Labor category mix for this task shall all be senior level (Tier 3) personnel and shall meet the certification and performance requirements listed below. This shall be identified in proposals as part of the proposed staffing approach.

NOTE: Each labor category proposed for this section shall hold and maintain the following certifications

- CompTIA Security plus- IAT Level II certification (All Personnel)
- Cisco Certified Network Professional
- Cisco Certified Network Professional Wireless
- Cisco Certified Network Professional Data Center

5.1.1 PERFORMANCE TASKS

a. Provide end-to-end troubleshooting of MARFORRES network infrastructure, to include data center infrastructure, wireless solutions, Network Access Control (NAC) solutions (802.1x), and Network Device Management (AAA) systems.
b. Provide technical expertise and proficiency in routing protocols, Dynamic Multipoint Virtual Private Network (DMVPN) technology (L3VPN), Cryptography (IPSEC), WAN Accelerators, NAC, AAA, and WLAN architecture.
c. Provide Network Administration, design, and engineering support including enterprise level wide area network (WAN) routing, data center infrastructure, quality of service, and access control list design, providing input on current and future projects and recommendations on system improvements across the section's area of responsibility.
d. Coordinate with circuit managers, providers, Base Telecommunication personnel, other Marine Corps organizations, and local touch labor as required to deliver and troubleshoot circuits and extensions, including both classified and unclassified networks.
e. Support Marine Forces Reserve's fully converged Voice/Video/Data network which includes a dual hub and spoke Dynamic Multipoint Virtual Private Network (DMVPN) topology covering multiple remote sites, developing, planning, drafting, and implementing design recommendations via approved change requests as necessary to modernize and improve the MARFORRES network infrastructure.
f. Design, implement, and manage modern, secure, and high availability data center infrastructures at the MARFORRES primary and alternate data center (Camp Lejeune, North Carolina.
g. In close coordination with MITSC-Reserve Server Administration, implement, operate, and maintain the LAN, SAN and Data Center unified fabric data center infrastructure.
h. In close coordination with MITSC-Reserve Server Administration, troubleshoot the LAN, SAN and Data Center unified fabric data center infrastructure as required.
i. Support the network infrastructure related to Marine Forces Reserve's Continuity of Operations Plan (COOP) and High Availability/Disaster recovery in the primary and alternate locations; developing, planning, drafting, and implementing design recommendations via approved change requests as necessary to modernize and improve the infrastructure. Average of 7 changes request per month.
j. Participate in all monthly and emergency service migrations, and provide after action reports to Government Team Lead within three business days.
k. Manage, administer and maintain the MARFORRES Network Access Control (NAC) solution and Network Device Management (AAA) systems and/or MITSC-Reserve controlled portions of the future enterprise solutions for these systems.

l. Provide NAC subject matter expertise administering and maintaining NAC and Network Device Management Authentication, Authorization and Accounting (AAA) systems for the Network Administration section.
m. Via the NAC solution, deliver network layer visibility and control of devices connecting to the MCEN-N & MCEN-S.
n. Via the Network Access Control (NAC) solution, secure MCEN-N & MCEN-S at the switch port by authenticating devices with 802.1X authentication.
o. Via the NAC solution, provide continuous monitoring capability & enforce EUD compliance.
p. Via the NAC solution, provide quarantine capability for EUDs failing authentication, compliance or remediation.
q. Via the NAC solution, report EUDs (End Users Devices) via Remedy Trouble Ticket Assigned to Triage failing authentication and remediation.
r. Provide Wireless Local Area Network (WLAN) subject matter expertise. Administer and maintain wireless systems for Network Administration.
s. Operate and maintain MITSC-Reserve controlled portions of the Marine Corps Enterprise Network Non-Classified (MCEN-N) WLAN solution.
t. Coordinate End User Device (EUD) connections to MCEN-N WLAN infrastructure with MCEN-N WLAN users and programs of record including troubleshooting Network Access Control as required.
u. Integrate EUD additions to MCEN-N WLAN, managing VLAN integration and SSID assignment as necessary.
v. Coordinate required workstation certificates for EUD wireless authentication with MCCOG, MITSC-Reserve Information Technology Endpoint Support, and Network Administration Network Access Control subject matter expert as required.
w. Execute and or assist the troubleshooting of MCEN-N WLAN system within the MITSC-Reserve area of operations, coordinating with the MCCOG and local base touch labor support as required.
x. Submit MCEN-N WLAN incident tickets and work orders via Remedy to support reporting and troubleshooting procedures.
y. Provide Tier III level support for escalated or high priority outage tickets including the WLAN, NAC and all portions of the network architecture supported by MITSC-Reserve Network Administration. An incident is an unplanned interruption to or quality reduction of an IT service. The service level agreements (SLA) define the agreed-upon service level between the provider and the customer. An incident ticket is used to track incidents. A work order is a formal request to carry out a defined activity. Work order tickets are used to service requests. Historical information indicates approx. 4 incident tickets per month and approx. 30 WO per month for Tier III.
z. Execute travel to remote sites to resolve high priority outages or issues on short notice as required (anticipate to average once per month or less).
aa. Execute after-hours maintenance as required. Typically, between the hours of 1800 - 2100, or as required. Normal maintenance nights are Tuesday and Thursday. The Government typically does not try to schedule technicians for more than one maintenance evening per week. At times, the maintenance windows may be scheduled outside of Tuesday and Thursday. Weekend maintenance may occasionally be required.
bb. Design overview documents, to include, Network Diagrams, Executable change requests with tasks detailing actions required to reach project completion, and configuration builds for network devices involved.
cc. Make Internet Protocol (IP) requests and updates to relevant departments as necessary for projects, including WLAN implementation IP information as required.

dd. Provide technical support for the Marine Corps Enterprise Network (MCEN) end-state solution for Core/Wide Area Network (WAN)/Base Area Network (BAN)/Local Area Network (LAN) architecture (Network Transition or Unification Project).
ee. Provide general network administration support utilizing network administration tools and applications
ff. Support and maintain network monitoring utilizing applicable software in either direct support or in coordination with enterprise support.
gg. Support Cybersecurity compliance through operational directive response, network authorization and accreditation requirements, Command Cyber Readiness Inspection, and cybersecurity incident response as required, providing all necessary documentation and information to the Network Administration Cybersecurity Liaison or MARFORRES Cyber Security.
hh. Provide technical support to ensure compliance with Cybersecurity directives and policies to include standing portions of inspections as required.
ii. Complete DISA STIG checklists and support Cybersecurity related inspections as required to ensure compliance with all applicable directives and policies. Conduct on average 1-2 STIG checklist reviews per year, or as needed for inspections, change requests, or Cybersecurity self-assessments. Completed DISA checklists are a deliverable. Execute the task or tasks in accordance to the Plan of Action and Milestone requirements for Cybersecurity packages as required by the Government Team Lead.
jj. Analyze, plan, and perform hardware and software upgrades/reconfigurations as required by manufacturer and supervisor to maintain vulnerability free network equipment at appropriate firmware and software versions.
kk. Provide technical expertise in all phases of equipment/application life cycles beginning with initial planning and feasibility analysis through implementation and enhancements; to include developing recommendations for, planning, and executing technical refresh of network equipment in coordination with the Network Administration Lifecycle Management specialist and the MITSC-Reserve Operations Technical refresh Project Manager.
ll. Provide support as required for technical refresh of network infrastructure.
mm. Provide technical support for High Availability Internet Protocol Encryptors (HAIPE) for classified environments.
nn. Provide Comsec key support and troubleshooting on High Availability Internet Protocol Encryptors as required.
oo. Provide reports to identify the health, reliability, degradation, and performance of the network environment to include capacity management related reports and availability management reports.
pp. Make recommendations and requests for circuit increases or upgrades based on capacity management reports or other related troubleshooting.
qq. Provide ad hoc technical documentation regarding the network environment in the conduct of daily tasks.
rr. Provide informal technical training vignettes on network equipment and best practices to Marines and civilians working in the G6 as required or requested.
ss. Provide on the job training to new government staff both military and civilians on network administration tools, systems, and processes.
tt. Follow all MITSC-Res Information Technology Library (ITIL) processes, procedures, and reporting requirements at all times. Recommend improvements as necessary to enhance continual process improvement efforts.
uu. Update trouble tickets, service requests and reply to emails within the timeframes required by MARFORRES ITIL processes and Standard Operating Procedures (SOP).
vv. Provide updates to SOPs as required.

ww. Participate in annual SOP reviews as required by Continual Process Improvement efforts within MARFORRES Network Administration.
xx. Complete assigned Change requests by the required primary completion dates with approved exceptions with Government Team Leads.
yy. Support the Marine Forces Reserve white line node (a Commercial ISP).
zz. Support the Marine Forces Reserve RCUN (tactical VRF) node as necessary.
aaa. Support the Deployed Site Transport Boundaries (DSTB) as necessary.

5.1.2 TASK AREA DELIVERABLES

TASK	DELIVERABLE	DETAILS	FORMAT	DUE DATE
5.1.1.ii	Complete DISA STIG Checklist	Complete DISA STIG checklists and support Cybersecurity related inspections as required to ensure compliance with all applicable Cybersecurity directives and policies.	CRQ or Self-assessments	1-2 reviews per year for regular updates are typical or as required for inspections
5.1.1.oo	Health, reliability, degradation, and performance of the network report	Provide reports to identify the health, reliability, degradation, and performance of the network environment to include capacity management related reports and availability management reports.	These reports will be pulled from a variety of sources and compiled into the Network Operations Brief (power point format)	Every two weeks
5.1.1.qq	Network environment report	Provide ad hoc technical documentation regarding the network environment as required.	Depends on the report needed, but can be an excel document or power point document.	Ad Hoc; On average one (1) to two (2) times a year a report in word format will be required
5.1.1.ss	New Staff Training	Provide on the job training to new government staff both military and civilians on network administration tools, systems, and processes.	Power Point.	Ad Hoc and Once per month.

5.2 Database Management and Maintenance

General Overview

Ensure the full mission capability by providing support to Marine Force Reserve (MFR) enterprise databases. Maintain, sustain, and upgrade current databases. Build and create new databases as required by application owners with approval of government lead. Generate complex queries and reports in support of software development. Perform database tuning, software patches, upgrades, and database monitoring. Assist in troubleshooting hardware and software problems related to databases and perform corrective actions. Provide technical support to ensure compliance with Cybersecurity directives and policies. Below outlines the current operating environment for this task area:

- Microsoft SQL Servers (40+) in two data centers on three separate networks.
- Server Size: 12 CPUs, 24GB of RAM, with 3 clusters.
- SQL Servers and databases span both unclassified and classified data.
- Three clusters in two data centers which are located in New Orleans, LA and Camp Lejeune NC.
- Eight availability groups in two data centers
- Seventy-six databases running in two data centers on three separate networks.
- Integrated with seven virtual centers in two data centers on three separate networks.
- Service migrations between both data centers monthly and as required by the commander due to natural disasters.
- Assist in the design and implementation of monthly, quarterly, and yearly patches on all servers and storage devices. Historically 3 cumulative patches since 2014.
- New Database deployment is based on the requirements of the applications developers.
- 76 Database are production only. The databases on the Dev/Test networks are counted separately, all under Microsoft SQL instances.
- Patching is based on the release of patches by Microsoft, average one patch per quarter.
- SQL Servers are currently being upgraded from 2014 to 2016.
- All Window Servers have been upgraded from 2012 to 2016, there are no Windows on 2008 R2 servers remaining in the MFR Data Center.
- After hours support is planned in advance to ensure any pitching/upgrades/maintenance is done to ensure no application outages. On-Call support, historically, has only been needed five times in the past year.
- Average five complex queries in a 12 month span.
- Support automatic interface of multiple external and internal databases into an organizational operational data warehouse, data mart platform for integration, SQL programming and subsequent provision to business intelligence platform components or other internal applications.

Minimum Certification Requirements

Below are the minimum certification requirements for this task area. The Labor category mix (i.e. senior, intermediate, and associate) to meet the certification and performance task requirements shall be identified in proposals as part of the proposed staffing approach.

NOTE: Each labor category proposed for this section shall hold and maintain the following certifications

- CompTIA Security plus- IAT Level II certification (All Personnel)
- MCSA - Microsoft Certified Solutions Associate in SQL Server 2012 or newer
- MTA - Microsoft Technology Associate Database Fundamentals

5.2.1 PERFORMANCE TASKS

a. Install, manage, and configure all Microsoft SQL servers.
b. Install, manage, and configure all SQL Clusters and Always-on-availability groups to ensure Continuity of Operations Plan is executable.
c. Manage and configure all SQL backups and maintain all backups per the standards set by government lead.
d. Generate complex queries and reports in support of software development efforts.
e. Generate custom queries as required to create new tables, views, and stored procedures in support of Power BI report development and data visualization.

f. Perform database tuning, software patches, upgrades and database monitoring.
g. Implement database standards policies and procedures
h. Participate in the development of application and database design standards to ensure consistency across all applications.
i. Maintain detailed database design documents, including products required for system certification and accreditation.
j. Participate in development of application and database design standards to ensure consistency.
k. Collaborate with MFR Software Engineers and SharePoint developers in support of optimized and efficient multiplatform solutions.
l. Participate in development of information technology continuity operations plan.
m. Participate in all monthly service migrations, emergency migrations, and provide after action reports to Government Lead within three business days.
n. Perform monthly and annually security reviews, perform DISA STIG review remediation, and provide periodic reviews on existing database documentation, all in accordance with Cybersecurity directives and policies.
o. Monitor SQL databases to assist leadership in determining corrective actions for all system errors.
p. Test backup and recovery process following the standard operating procedures to ensure that data can be successfully be retrieved.
q. Provide technical support to ensure compliance with Cybersecurity directives and policies.
r. Provide on the job training to new government staff both military and civilians for the use of the migration tools and SQL servers standard operating procedures.
s. Provide reports to identify the health, reliability, degradation, and performance of the SQL databases and backup environments.
t. Complete all Plan of Action and Milestone (POAM) requirements for all Cybersecurity accreditation packages. The ten plans of actions and milestones for the applications and the accreditation package is detailed but not complex.
u. Provide information to leadership for required hardware purchases, assist in the design and installation of any new database servers to ensure integration with all application servers.
v. Ad-hoc reporting will be required on average once every other month, low in complexity, and government lead will establish appropriate timeline based on complexity.
w. Using a common set of integrated and synthesized Force and local command data, tailor each dashboard to depict a common set of Force visualizations and those required by the local unit.
x. Incorporate drill down and interactive capabilities based on user interface requirements.
y. Identify, troubleshoot and resolve SQL related issues with PowerBI dashboards according to the following tiers:
    i. Tier 1 – 24-48 hours
    ii. Tier 2 – 24-96 hours
    iii. Tier 3 – 1-5 business days+ depending on scope and severity of issue established by supervisor and stakeholder
z. Generate detailed documentation on all SQL Queries and DAX/R/Python code used to create Power BI Reports, Dashboards, and visualizations along with any custom slicers, measures, calculated fields, etc.
aa. Develop products according to the Development Lifecycle consisting of:
    - **Minor Project**
    - Requirements Gathering – 1 week
    - Authoritative Data Source interface (where applicable) 1-2 weeks
    - Product Build Development – 2 weeks

- Testing and Validation – 1 week
- Product Delivery and Handoff – 1 week

- **Major Project**
- Requirements Gathering – 2 weeks
- Authoritative Data Source interface (where applicable) 1-2 weeks
- Product Build Development – 4 weeks
- Testing and Validation – 2 week
- Product Delivery and Handoff – 1 week

5.2.2 TASK AREA DELIVERABLES

TASK	DELIVERABLE	DETAILS	FORMAT	DUE DATE
5.2.1.i, s	Accreditation Package POAM	To include remediation, mitigation, status for all open vulnerabilities	Word or Excel document	Due to the COR or technical representative designated by the COR as required by each Accreditation package
5.2.1.l	Service Migration After Action	After action report after each service migration	Word or Excel document	Due to COR or technical representative designated by the COR within 3 business days of the Service Migration
5.2.1.c, o, r	Weekly Database Server Status Report	To include the health and reliability of backup /restore capabilities, consumption of hard drive on servers	Word or Excel document	Due to the COR or technical representative designated by the COR by 0800 every Monday.
5.2.1.u	Ad-hoc Reports	As needed by government team lead	Word or excel document	As agreed upon by government team lead

5.3 Server Administration

General Overview

Ensure full mission capability by providing support to Marine Forces Reserve (MFR) server and storage infrastructure. Provide support to design, install, configure, and maintain two data centers with a Continuity of Operations Plan (COOP). Provide onsite ability to troubleshoot hardware, software, physical and virtual servers, storage devices and the capability to backup and restore all systems. Integrate all servers with virtual software and storage devices. Analyze, plan, and perform hardware and software

upgrades/reconfigurations as required by manufacturer and Government Lead. Implement and maintain the Site Recovery Plan in regards to service migrations between two data centers in non-geographically located data centers to ensure the government's ability to avoid natural disasters. Provide technical support to ensure compliance with Cybersecurity directives and policies. Provide reports for hosts and virtual machine uptime, memory, and process utilization for all MFR network environments. Provide ad hoc technical documentation regarding the server environment. Below outlines the current operating environment for this task area:

- Physical Servers (63) – including but not limited to Five Cisco UCS Chassis with a minimum of twenty B200 M3/4/5 blades, nine HP ProLiant DL360 Gen8, and ten HP ProLiant DL380 Gen9 servers running in two data centers on four networks. Servers are located in various location, but all can be managed from Marine Forces Reserve, New Orleans.
- Virtual Servers (290+) - Windows Server 2016, Windows Server 2012, Windows Server 2008, Red Hat Linux, Linux 2.6x or newer, Debian, SUSE, and CentOS.
- Virtual Centers (7) – Integration with eleven server clusters on four networks.
- Storage devices - Eight NetApp heads, eighteen disk shelves, two Tegile shelves, two VSANs over ten physical hosts, with over 830 terabytes in storage in two data centers on four networks.
- VMWare 6.0 is running all hosts and manages. No other vendor is used for virtualization at this time.
- Other Server Administration Tools currently in use:
    i. Remote desktop
    ii. VMWare vSphere
    iii. VMWare Horizon
    iv. Remote Server Administration Tools (RSAT)
    v. NeTApp On-Command
    vi. VMWare Site Recovery Manager
    vii. NetApp Storage Replication Adapter
    viii. SnapCenter
- Other Software:
    i. VMWare Horizon
    ii. VMWare vSAN
    iii. NFS Storage integration with VMWare

Minimum Certification Requirements

The Labor category mix for this task shall all be senior level (Tier 3) personnel and shall meet the certification and performance requirements listed below. This shall be identified in proposals as part of the proposed staffing approach.

CompTIA Security plus- IAT Level II certification (All Personnel)
-VMWare Certified Professional 6.0DCV or newer
-Microsoft Certified Solutions Associate (MCSA) Windows Server 2012 or newer
-NetApp Certified Data Administrator, ONTAP
-NetApp Certified Storage Associate

5.3.1 PERFORMANCE TASKS

a. Install, manage, and configure all physical hosts.
b. Install, manage, and configure all VMWare software on physical hosts.

a. Currently VMWare 6.0 is running all hosts and manages. No other vendor is used for virtualization at this time

c. Install, manage, deploy, and configure all virtual servers in VMWare and on the physical hosts.
d. Integrate VMWare technologies with all storage providers.
e. Install, manage, and configure all filers.
f. Install, manage, and configure all migration software.
g. Assist in troubleshooting all physical and virtual platforms, to include but not limited to UCS, HP, Dell, and any other government procured hardware.
h. Provide on the job training to new government staff including military and civilians, for the use of the migration software and systems to include Virtual systems.
i. Monitor VMWare and Physical servers to assist leadership in determining corrective actions for all system errors.
j. Assist in troubleshooting all storage platforms to include but not limited to NetApp, Tegile, and any other government procured hardware.
k. Monitor storage platforms to assist leadership in determining corrective actions for all system errors.
l. Investigate hardware and software problems related to the storage and backup infrastructure and perform corrective actions.
m. Participate in all monthly service migrations, emergency migrations, and provide after action reports.
n. During critical hurricane months (June – November), provide four hour onsite support to complete an emergency migration, and provide after action reports.
o. Test backup and recovery process following the standard operating procedures to ensure that data can be successfully be retrieved on a quarterly basis.
p. Test migration plans weekly using Government provided software.
q. Investigate hardware and software problems related to the physical and virtual infrastructure and perform corrective actions.
r. Complete DISA STIG checklists and support Cybersecurity related inspections as required to ensure technical compliance. Provide technical support to ensure compliance with Cybersecurity directives and policies.
s. Provide reports to identify the health, reliability, degradation, and performance of the physical and virtual environments as well as the storage and backup environments.
t. Develop and or update server system security plan (SSSP) and the server and storage system design documents.
u. Work trouble tickets as assigned. Approximately 25 trouble tickets annually.
v. Assist in the design and implementation of monthly, quarterly, and yearly patches on all servers and storage devices.

5.3.2 TASK AREA DELIVERABLES

TASK	DELIVERABLE	DETAILS	FORMAT	DUE DATE
5.3.1.m	Service Migration After Action report	After action report after each service migration.	Word or Excel Document	Due to COR or technical representative designated by the COR within 3 business days of Service Migration.
5.3.1.r	Accreditation Package POAM	To include remediation, mitigation, status for all open vulnerabilities	Word or Excel Document	Due to the COR or technical representative designated by the COR as required by each Accreditation package.

5.3.1.l, s	Weekly Storage status report	To include consumption of volumes, status of backups, and Virtual Machine hard drive utilization.	Excel Document	Due to the COR or technical representative designated by the COR by 0900 every Monday.
5.3.1.s	Weekly Network Operations Slides	To include Physical and virtual host memory and CPU utilization, top CPU and memory virtual machines, consumption of volumes, and migration status.	Power Point	Due to the COR or technical representative designated by the COR by 1100 every Tuesday.

5.4 Telecommunication Maintenance

General Overview

Ensure full mission capability by providing Tier III senior level technical support to the Marine Forces Reserve (MFR) WAN/BAN/LAN serving the Marine Forces Reserve (MARFORRES) Headquarters at MARCORSPTFAC New Orleans, the command's alternate data center in Camp Lejeune, North Carolina, and 160 remote sites. Below outlines the current operating environment for this task area:

- Consists of approximately 1,000 Network devices at 160 sites and two data centers including both classified and unclassified networks. Nodes contain numerous base extensions both organically and externally supported dependent on remote site base status and any applicable memorandums of understanding.
- Two Data Centers built on Cisco Nexus and Unified Computing System (UCS) technology.
- Support the Marine Forces Reserve whiteline node (a Commercial ISP).
- Support the Marine Forces Reserve RCUN (tactical VRF) node as necessary.
- Support the Deployed Site Transport Boundaries (DSTB) as necessary.
- Current Network Devices and tools include but are not limited to: Cisco Catalyst 6500; Cisco Catalyst 4500; Cisco Catalyst 9300; Cisco Catalyst 3850; Cisco Catalyst 3750; Cisco Catalyst 3560; Cisco Nexus Devices; Cisco ASR 1002; Cisco ASR 1006; Cisco 2900 series routers; Cisco 3900 series routers; Cisco 4000 series routers; Cisco ISE with TACACS/Network Device Management Integration to include support for multifactor authentication; Aruba and HP wireless network infrastructure; Forescout CounterAct; High Assurance Internet Protocol Encryptors; Solarwinds Kiwi Tool suite; Riverbed Steelhead; GEM-X encryptor management system.
- High Availability Internet Protocol Encryptors for Classified environments including related Key Material.
- Network Common Operation Picture and Network Device Management is currently provided by: HP Network Node Manager I and HP Network Automation.
- Network Access control (NAC/802.1x) and Network Device Management is currently provided by: Cisco Identity Services Engine (ISE); TACACS+ via Device Administration License in Cisco ISE.
- Network Access control (NAC/802.1x) is moving to: Forescout Counteract.
- Backup Network Configuration automation is provided by: Kiwi Cattools.

- Log management is currently provided by Kiwi Syslog, moving to enterprise McAfee SIEM solution.
- WAN accelerators are currently Riverbed models.
- DHCP Servers are running on Windows servers.
- Redseal, DISA ACAS and STIG Checklists are primary used to ensure compliance with Cybersecurity directives.
- Alternate data center is currently located on Camp Lejeune, NC. Alternate site must provide equivalent services and support to all end users, as primary site.
- Specific telecommunications requirements for alternate site differ from that of the data center layout and site architectures differ.
- Telecommunication services are primarily provided via requests to the Camp Lejeune Base communications office.

Minimum Certification Requirements

Below are the minimum certification requirements for this task area. The Labor category mix (i.e. senior, intermediate, and associate) to meet the certification and performance task requirements shall be identified in proposals as part of the proposed staffing approach.

NOTE: Each labor category proposed for this section shall hold and maintain the following certifications

- CompTIA Security Plus- IAT Level II Certification (All Personnel)
- Cisco Certified Network Professional

5.4.1 PERFORMANCE TASKS

a. Provide end-to-end troubleshooting of MARFORRES network infrastructure, to include coordinating with circuit managers, providers, Base Telecommunication personnel, other Marine Corps organizations, and local touch labor as required to deliver and troubleshoot circuits and extensions, including both classified and unclassified networks; and local touch labor as required to deliver and troubleshoot circuits, extensions, and troubleshoot inside/outside plant wiring, cabling, and patching, including both classified and unclassified networks.
b. Provide Tier III level support for escalated or high priority outage tickets with a focus on troubleshooting inside plant/outside plant issues in coordination with local site POCs, local Base Communications offices (where applicable) and service providers/LECs.
c. Support the Marine Forces Reserve whiteline node (a Commercial ISP).
d. Support the Marine Forces Reserve RCUN (tactical VRF) node as necessary.
e. Support the Deployed Site Transport Boundaries (DSTB) as necessary.
f. Execute travel to remote sites to resolve high priority outages or issues on short notice as required (anticipated to average once per month or less).
g. Plan, execute, and document site transitions from MCEN-N (COINS) to MCEN-N (RNET) networks.
h. Provide technical support for the NGEN end-state solution for Core/Wide Area Network (WAN)/Base Area Network (BAN)/Local Area Network (LAN) architecture (Network Transition or Unification Project).
i. Plan, execute, and document Information Technology Infrastructure Projects (ITIP) to meet validated requirements for network infrastructure additions or for new site installations.
j. Recommend and request Circuit orders from the MARFORRES Circuit Management Office as necessary.

k. Plan, coordinate, schedule and execute circuit extensions and activations in coordination with service providers and the MARFORRES Circuit Management Office, to include coordinating/delivering circuit extensions with local Base Communications offices or Marine Forces Reserve Facilities office as necessary.
l. Provide technical expertise and proficiency in Cisco Enhanced Interior Gateway Routing Protocol (EIGRP) and Border Gateway Protocol (BGP) routing protocols, Dynamic Multipoint Virtual Private Network (DMVPN) technology (L3VPN), Cryptography (IPSEC), WAN Accelerators, to include maintenance of network equipment to appropriate firmware and software versions.
m. Support Marine Forces Reserve's fully converged Voice/Video/Data network which includes a dual hub and spoke Dynamic Multipoint Virtual Private Network (DMVPN) topology covering multiple remote sites, developing, planning, drafting, and implementing design recommendations via approved change requests as necessary to modernize and improve the MARFORRES network infrastructure.
n. Support the network infrastructure related to Marine Forces Reserve's Continuity of Operations Plan (COOP) and High Availability/Disaster recovery in the primary and alternate locations, developing, planning, drafting, and implementing design recommendations via approved change requests as necessary to modernize and improve the infrastructure.
o. Provide Telecommunications Engineer design or input on system improvements across the section's area of responsibility.
p. Provide support utilizing network administration applications.
q. Support and maintain network monitoring utilizing applicable software.
r. Support operational directive response, network authorization and accreditation requirements, Command Cyber Readiness Inspection, and cybersecurity incident response as required, providing all necessary documentation and information to the Network Administration Cybersecurity Liaison or MARFORRES Cyber Security.
s. Complete DISA STIG checklists and support Cybersecurity related inspections as required to ensure technical compliance to all Cybersecurity directives and policies.
t. Provide technical expertise in all phases of equipment/application life cycles beginning with initial planning and feasibility analysis through implementation and enhancements; to include developing recommendations for, planning, and executing technical refresh of network equipment in coordination with the Network Administration Lifecycle Management specialist and the MITSC-Reserve Operations Technical refresh Project Manager.
u. Provide support as required for refresh of network infrastructure.
v. Provide expertise to support and assist in developing policies, procedures, and major programs for MARFORRES, including but not limited to: NGEN, SONIC, Multi-Protocol Label Switching (MPLS), Marine Corps Enterprise Network (MCEN) Point of Presence (POP) suite, Voice Over IP (VOIP and VOSIP), Virtual Desktop Infrastructure (VDI), Port Administration/Security and Network Access Control, Compliance, and Remediation (NACCR), and Marine Corps Enterprise Network Non-Classified Internet Protocol Router Network Wireless Local Area Network.
w. Create reports to identify the health, reliability, degradation, and performance of the network as required.
x. Provide ad hoc technical documentation regarding the network environment as required.
y. Provide technical training vignettes on network equipment and best practices to Marines and civilians working in the G6 as required.
z. Provide on the job training to new staff on network administration tools, systems, and processes.
aa. Update trouble tickets, service requests and reply to emails within the timeframes required by MARFORRES ITIL processes and Standard Operating Procedures (SOP). Provide updates to

SOPs as required. Participate in annual SOP reviews as required by Continual Process Improvement efforts within MARFORRES Network Administration.

bb. Follow all MITSC-RES ITIL processes, procedures, and reporting requirements at all times.

cc. Complete assigned Change requests by the required primary completion dates with minimal exceptions for unusual circumstances

5.4.2 TASK AREA DELIVERABLES

TASK	DELIVERABLE	DETAILS	FORMAT	DUE DATE
5.4.1	Participation in daily standup and end of day summary with Tier Lead, providing updates on all currently assigned tasks	Informal daily meeting.	Word/excel/power point. Verbal presentation.	Daily
5.4.1.q	Monthly rollups from the contractor office detailing work	Monthly accomplishments	Word Document	Monthly

5.5 Software Engineering

General Overview

REVISED PARAGRAPH: Provide comprehensive development, operational, and maintenance support to MARFORRES web based application systems including Individual Ready Reserve (IRR), Memorandum Fiscal Services (MFS), Training, Exercise and Employment Program, Transportation of People, and Transportation of Things (T3), and MFR Manpower, as well as develop and support new web based applications for MARFORRES by leveraging the Agile Development process. Below is brief description of each of the current applications.

MFS is the primary MARFORES financial system used to integrate diverse data from external systems. MFS delivers a wide span of support covering multiple functional areas within the MARFORRES financial community such as the following: budgeting support, authorization funding management, conference request routing, unit travel card processing, transactional research/validation, financial reporting, billing reconciliation, Defense Travel System account management, and evaluation assessments. MFS is a web based system supporting more than 500 active users throughout the continental United States in support of the MARFORRES financial community. MFS is an ever-evolving financial tool designed to provide accurate and expedient budgeting and accounting information to assist managers in making informed decisions effecting the command's financial posture. With Business Process Reengineering as the main focus of MFS, the system is designed to fill capability gaps, automate and streamline workflows, and provide integrated reporting capabilities. MFS is agile and able to adapt quickly to the changing DoD financial landscape as new requirements and policy changes must be incorporated into the system to ensure compliancy. MFS is a primary facilitating system for MARFORRES in audit support by offering document retention and rapid retrieval capabilities. MFS has three major external data feeds and two additional internal data exchanges which are processed daily from these Marine Corps systems: SMARTS, MROWS, and GCSS-MC. Currently there are 4 data exchanges, 3 are one-directional (incoming) and one interface is bi-directional. Once the data is received, MFS runs an integration processing job to prepare this data for

end users every morning. On average annually, the MFS programming cycle includes 3-4 major projects (greater than two weeks design phase – 4 weeks in the development phase) and roughly 8 minor projects (under two weeks in duration). The new development requirements range from cosmetic modifications to major modular rewrites based on the prioritization of the MARFORRES MFS Configuration Control Board. In addition, there are several items that fall outside of the normal System Development Life Cycle that require support such as: COOP preparation, ADHOC reporting support, system/network troubleshooting, and tasks required to maintain the system's Authority to Operate (ATO). The contractor should be familiar with T-SQL DB and ASP.NET Web Forms in VB to work within the MFS program.

T3 is a web based system designed to be a Commander's TEEP management and transportation management tool, capable of identifying unit, personnel, equipment, and resources prior to the execution of training exercises or deployments COMMARFORRES is responsible for the training and the operational readiness of 39,000 Marine Reservists. MARFORRES G-3/5 is responsible for managing a financial database that integrates Operating Budgets with training and exercises, which result in resource utilization over time. Resources are defined as units and their associated personnel, equipment, and funding. The MARFORRES G-3/5 Department provides budgeting, accounting, execution and financial support services through the T3 Database to four Major Subordinate Commands (4th Marine Aircraft Wing, 4th Marine Division, 4th Marine Logistics Group, and the Force Headquarters Group) in addition to many major programs managed at the headquarter level. A major challenge facing the MARFORRES G-3/5 is the geographical dispersion of the more than 160 sites throughout the United States.

The MFR IRR Management Application is a web based system designed to maintain accurate and current personnel records on members of the Individual Ready Reserve Components, to include mailing address, physical condition, military qualifications, dependency status, civilian occupational skills, availability for service, and other information that is needed to determine strength levels of the Military Services. Below outlines the current operating environment for this task area:

Currently Microsoft Visual Studio is used to develop the code, and Azure DevOps server for version control, testing and release management capabilities. The development team in coordination with the Marine Forces Reserve Server/Network personnel to conduct the user acceptance testing, performance, and load testing of the applications. Release notes are published to the home page of each application. Currently there are no set monthly release scheduled for changes to production. In the current environment MFR follows an agile schema, sprints are anywhere from 2-6 weeks, and depends on the complexity of the project.

The demands on each application translate to a functionality backlog of 50-100 items varying in levels of complexity. Each program manager operates on a continuous agile development schedule producing new functionality at least once a month. Our software engineers receives roughly on average of 10 tickets per month; most are for minor bugs or cosmetic changes. Non "bug" tickets are required to be presented to each applications Configuration Control Board (CCB). Out of the 10 tickets, about 2-3 requests per week ranging from simple bug fixes or cosmetic adjustments; major rewrites range from about (1-2 per year). Each application must also be updated to meet current technology platform changes which equate to major re-writes every three years on average.

MFS has roughly 500-600 active daily users, T3 has approximately 300 active daily users, and MFR Manpower has approximately 200. MFS has right at 150,000 lines of code, while MFR Manpower has approximately 12,000; T3 system has approximately 100,000. In addition to the number of lines of codes, each system has a code quality range, which ranges from adequate to exceptional. These are mature systems which needs to be maintained while at the same time prepare to update to new technologies and help develop new features. Below outlines the current operating environment for this task area:

Minimum Certification Requirements

Below are the minimum certification requirements for this task area. The Labor category mix (i.e. senior, intermediate, and associate) to meet the certification and performance task requirements shall be identified in proposals as part of the proposed staffing approach.

NOTE: Each labor category proposed for this section shall hold and maintain the following certifications

- CompTIA Security+ (All Personnel)
- Experience in:
    i. Risk Management Framework (RMF) accreditation process
    ii. Enterprise application management
    iii. Software development change management.
    iv. Code development in web-based and Model-View-Controller programming languages (applicable only to personnel supporting IM/KM under task area 5.5)
- Microsoft 70-461 test querying MS SQL Server 2012/2014

5.5.1 PERFORMANCE TASKS

a. Apply process improvement, reengineering methodologies, and internet-related methodologies and principles to conduct process modernization projects incorporating best practices and preparing/delivering milestone status reports as part of quality assurance.
b. Provide support to develop Web based applications including complex queries and stored procedures to transform government agencies to be able to deliver their services on time. Provide support in developing the site concept, interface design, and architecture of the web-site. Provide support for the implementation of interfaces to applications.
c. Build and deploy end user reporting requirements. Establish report definitions and permissions to include ADHOC reporting to satisfy time-sensitive data calls.
d. Build and maintain data integration packages to accommodate external data sources to include scheduling of data transfer along with preparation of the supporting Interface Connection Agreement (ICA) documentation.
e. Evaluate, recommend, and implement automated test tools and strategies as well as manage test environment account permissions. Testing is conducted on the Marine Forces Reserve Cyber Node.
f. Coordinate and test Electronic Data Interchanges with DISA for modifications and new implementation initiatives.
g. Provide technical recommendation for leveraging emerging technology in adherence with governmental policy and regulations.
h. Ensure all requirement system specifications are fully functional, properly implemented, and secure.
i. Provide assistance and training to users accessing the system and prepare instructional material to support functionality.
j. Create, monitor, and optimize data transfers to/from external origins for scheduling and maintenance.
k. Analyze user interfaces, maintain hardware and software performance tuning, analyze workload and computer usage, maintain interfaces with outside systems, analyze downtimes, and analyze proposed system modifications, upgrades and new COTS.

l. Monitor and evaluate system database usage and performance metrics/statistics and apply new technologies and programs for optimization.
m. Identify and troubleshoot problems and coordinate with the Government Lead to ensure problems are resolved to the users' satisfaction.
n. Recommend and advise Government Team Lead on system improvements/problem resolution in areas relating to architecture, network, communication, protocols, risk management, and development methodologies.
o. **Develop** outlines and drafts for review and approval by technical specialists and project management ensuring that final documents meet applicable governmental requirements and regulations.
p. Prepare required documentation to include technical documents, functional descriptions, system specifications, guidelines, instructional material, security requirements, user manuals, **configuration** documents, and operational procedure manuals in support of routine **develop**ment and in maintaining the system's Authority to Operate (ATO). Currently HP Fortify is used as the primary Application Security product. MFS ATO is valid until April 2021.
q. Provide support as required outside the scope of the traditional system development life cycle such as: preparing records for destruction in accordance with record management policy, executing the Continuity of Operations Plan (COOP), and assist in Knowledge Management strategies.
r. **Execute the service migration (COOP). The first Thursday of each month requires the migration of services between Camp Lejeune, NC and New Orleans. Required to assist after hours and to verify system services have been properly restored. System must be fully operational and reported to the COR the following work day.**
s. Integrate all designs with Team Foundation Server and Configuration Control Board efforts to maintain awareness and system documentation requirements.
t. Provide clear, efficient communication with customers and stakeholders during requirement gathering, development, product delivery, and support cycles.
u. Provide collaborative support as required to interface MARFORRES applications with Power BI to provide near real-time report capabilities for MARFORRES systems.
v. Support interface connection agreements between MARFORRES applications and external data sources.
w. Generate complex queries and reports in support of software development efforts.
x. Maintain detailed documentation on Dashboard, Dataset, and Data Model design.
y. Build and maintain data integration packages to accommodate external data sources to include scheduling of data transfer along with preparation of the supporting Interface Connection Agreement (ICA) documentation.
z. Maintain adherence to DOD and MFR Cyber Security standards regarding PII/FOUO sensitive data, data aggregation classification, and product access permissions assignments
aa. Generate detailed documentation on all SQL Queries and DAX/R/Python code used to create Power BI Reports, Dashboards, and visualizations along with any custom slicers, measures, calculated fields, etc.
bb. Integrate all designs with Team Foundation Server and Configuration Control Board efforts to maintain awareness and system documentation requirements.
cc. Develop products according to the Development Lifecycle consisting of:
    - **Minor Project**
    - Requirements Gathering – 1 week
    - Authoritative Data Source interface (where applicable) 1-2 weeks
    - Product Build Development – 2 weeks
    - Testing and Validation – 1 week

- Product Delivery and Handoff – 1 week

- **Major Project**
- Requirements Gathering – 2 weeks
- Authoritative Data Source interface (where applicable) 1-2 weeks
- Product Build Development – 4 weeks
- Testing and Validation – 2 week
- Product Delivery and Handoff – 1 week

5.5.2 TASK AREA DELIVERABLES

TASK	DELIVERABLE	DETAILS	FORMAT	DUE DATE
5.5.1.b, o, p	System change control documentation	Supporting documents for all system development to include: Requirements, Design, Development, and Testing documentation.	Word or Excel document.	Due to the COR NLT 5 working days post release.
5.5.1.o, p	Provide system documentation	Updates to specific system-related documents to include version control for the Configuration Control Plan, Security Plan, Boundary Diagrams, System Connection Agreements, system Design documents and other documentation as may be required by external data calls.	Word or Excel document.	Due to the COR as requested.
5.5.1.o, p	Accreditation Package POA&M	State remediation, mitigation status for all open vulnerabilities.	Word or Excel document.	By established due date. All milestone and control dates must be met and reported to MFR Cybersecurity Branch.

5.6 SharePoint Development and Administration

General Overview

Responsible for the design, implementation, development, maintenance and support of the current and future. MFR SharePoint intranet platform. Ensure the quality, stability and performance of existing sites, applications and solutions. SharePoint is an essential solution for MARFORRES in that it provides a secure, manageable, web-based collaboration platform supporting more than 15,000 active users located throughout the continental US in support of Marine Forces Reserve. The contractor should possess

exceptional time and project management skills, as well as understanding of developing, customizing and deploying SharePoint solutions using SharePoint Designer, SharePoint Foundation, Microsoft SQL databases, Microsoft Power BI, VB.Net (Visual Basic) applications, ASP.NET/C# applications, and ASP.NET MVC. In addition, the contractor must be able to support the testing process, data integration, risk management analysis, technical wring, record management, and supporting the Continuity of Operations Plan (COOP). Solutions provided must be delivered efficiently while meeting established standards, regulations, and guidelines for MFR and DoD operational IT systems. Below outlines the current operating environment for this task area:

- MFR IM/KM currently has a robust SharePoint environment consisting of 32 site collections with approximately 30 sites, dozens of SharePoint solutions, workflows, and numerous pages per collection. This always-on availability environment supports close to 100,000 users and encompasses upwards of 1.5TB of SharePoint Data that interfaces with Power BI which provides programmable, near real-time reporting solutions for numerous SharePoint solutions. On average annually, IM/KM programming cycle includes 3-4 major projects (greater than four weeks in the development phase) and 8 minor project (under two weeks) that range from cosmetic modifications to other minor recommendations due to business process changes or new review/approval workflows. In addition, there are several items that fall outside of the normal SDLC that require support such as COOP preparation, system/network troubleshooting, etc. Most of the custom development is out of the box solutions, with several JavaScript and CSS custom solutions. These applications are classified as Mission Assurance Capable (MAC) II systems and require immediate response to any outage. These applications MUST be operational 24/7/365, with optimal speed and reliability, while continuing to develop and update them. Due to high turnover rates in the military, the Contractor will also be responsible for conducting 3-4 week-long user training sessions annually.
- MCCAST is a custom RMF tool created for the USMC.

Minimum Certification Requirements

Below are the minimum certification requirements for this task area. The Labor category mix (i.e. senior, intermediate, and associate) to meet the certification and performance task requirements shall be identified in proposals as part of the proposed staffing approach.

NOTE: Each labor category proposed for this section shall hold and maintain the following certifications

- CompTIA Security+ (All Personnel)
- Minimum 3 Years of experience in development of SharePoint environment

5.6.1 PERFORMANCE TASKS

a. Ensure full mission capability by providing support to MARFORRES SharePoint site and Microsoft's Internet Information Server (IIS) consisting of development and production versions of (a) Microsoft Office SharePoint Server (MOSS) (currently MOSS 2013, migrating to SharePoint 2016 and Office 365), Microsoft Power BI Report Server, and Internet Information Services (IIS).
b. Plan, direct and coordinate the preparation, implementation and management of long-term SharePoint administrative operations; and, provide diagnosis, identification, and resolution of problems with hardware, software, and interfaces.

c. Provide customer assistance, troubleshooting, configuration, and knowledge management activities in response to customer inquiries within 14 business days.
d. Assess customer requirements and document using existing organizational requirements documentation processes.
e. Conduct periodic hardware or software maintenance in accordance with engineering guidance.
f. Participate in meetings and technical work groups as needed providing consultation regarding SharePoint related issues.
g. Assist in recovering data upon customer request.
h. Design and improve the site collection architecture as required on an ad hoc basis.
i. Conduct requirement analysis and development of customized SharePoint solutions leveraging all out of the box SharePoint capabilities to include java script, HTML, and .net code. Solution delivery will include user training, document, and sustainment plans.
j. Design and implement SharePoint sites and pages to integrate Power BI reports and dashboards within SharePoint and M365/SharePoint Online architectures.
k. Assist in the design and development of customized, integrated Power BI solutions.
l. Participate in development of applicable portions of the MARFORRES Continuity of Operations Plan (COOP).
m. Provide remediation when SharePoint & IIS infrastructure is found to be noncompliant with STIG checklist. Apply patches within 14 days of release and update Plan of Action & Milestones (POA&M) items as necessary.
n. All MITSC-RES ITIL processes and procedures shall be followed.
o. Provide on-call support (i.e. responding to submitted trouble tickets during regular working hours). (Average 60 tickets per year acknowledge within 36 business hours and resolve in 14 business days.)
p. Provide design assistance to department site owners who create web content, to include SharePoint and Power BI Report design assistance.
q. Operate in an agile development environment.
r. Remediate all findings prior to the established due dates for outstanding controls listed on the Risk Management Framework (RMF) and STIG Plan of Action & Milestones (POA&M). POA&M tracking on SharePoint page must be kept up to date. Requests for extensions must be submitted through the Remedy system prior to due date expiring.
s. Provide training on SharePoint and Power BI to end users and site administrators. Training will consist of at least four on site classes at various locations across the country, a virtual classroom environment hosted on the SharePoint including student sandbox.
t. Maintain and manage a MFR SharePoint Site Owner certification distance learning course.
u. Manage MFR SharePoint Oversight Council conducting quarterly user meetings, webinars, and town hall meetings to discuss and improve user awareness and user experiences.
v. Perform all actions required to support the Authority to Operate (ATO) on DoD networks, which includes completing the Risk Management Framework (RMF) package provided by the USMC. Actions required for subsequent re-approval must be accomplished prior to established due dates (usually every three years).
w. Provide support for annual approval of the applications in the Department of Defense Information Technology Portfolio Repository-Department of the Navy (DITPR-DON) annual record review. This requires completing a Privacy Impact Assessment (PIA) and a Clinger-Cohen Act (CCA) Compliance Table that will be provided by the USMC. Annual approval due date is during the February-March timeframe.
x. Perform all actions required to support the Authority to Operate (ATO) on DoD networks, which includes completing the Risk Management Framework (RMF) package provided by the USMC.

y. The contractor should understand the RMF process, as it will be the responsibility of the contractor to collect artifacts and input them into MCCAST.
z. Actions required for subsequent re-approval must be accomplished prior to established due dates (usually every three years).
aa. Develop and manage the enterprise approach to permission management in accordance with SharePoint best practices and DOD PII and Cyber security requirements.
bb. Develop and manage the enterprise approach to SharePoint governance to include naming conventions, metadata tagging, and management of the term store.
cc. Design integration plan for SharePoint and M/O365, and Power BI across all business areas including, but not limited to, manpower, administration, logistics, communications, operations, training, medical, fiscal, and facilities.
dd. Develop effective SharePoint based dashboard access/permissions using a common set of integrated and synthesized Force and local command data; tailor each dashboard to depict a common set of Force visualizations and those required by the local unit.
ee. Integrate dashboards into MFR SharePoint, and SharePoint Online ensuring accessibility from all government devices via CAC.
ff. Generate User Experience (UX) and User Interface (UI) standards to facilitate dashboard creation and integration
gg. Maintain detailed documentation on SharePoint/dashboard integration, datasets, and Data Model designs.
hh. Develop embedded dashboard access/permission request workflows.
ii. Generate and update IM/KM governance for SharePoint and Power BI integration efforts to include permissions management hierarchies.
jj. Develop products according to the Development Lifecycle which consists of:
    - **Minor Project**
    - Requirements Gathering – 1 week
    - Authoritative Data Source interface (where applicable) 1-2 weeks
    - Product Build Development – 2 weeks
    - Testing and Validation – 1 week
    - Product Delivery and Handoff – 1 week

    - **Major Project**
    - Requirements Gathering – 2 weeks
    - Authoritative Data Source interface (where applicable) 1-2 weeks
    - Product Build Development – 4 weeks
    - Testing and Validation – 2 week
    - Product Delivery and Handoff – 1 week

5.6.2 TASK AREA DELIVERABLES

TASK	DELIVERABLE	DETAILS	FORMAT	DUE DATE
5.6.1.c	Risk Management Framework (RMF)	Required to support the Authority To Operate (ATO) on DoD networks, and required for subsequent re-approval	Provided by the COR	Must be accomplished prior to established due dates (typically every two or three years)
5.6.1.u	Privacy Impact Assessment (PIA) and annual	Support for the annual approval of the applications in the Department of Defense	Provided by the COR	Due annually during Feb-Mar timeframe

	Clinger-Cohen Act (CCA) Compliance Table	Information Technology Portfolio Repository-Department of the Navy (DITPR-DON) annual record review		
5.6.1.k	Apply patches and update Plan of Action & Milestones (POA&M) items as necessary.	Required to install software patches, and update Plan of Action & Milestones (POA&M) documents as necessary.	Provided by the COR	Within 14 days of release & as required
5.6.1.i	Conduct requirement analysis and development of customized SharePoint solutions	SharePoint capabilities to include java script, HTML, and .net code	User training, document, and sustainment plans format provided by COR	Adhoc

5.7 IT Operations and Maintenance Program Management

General Overview:

Plans, directs, and coordinates a cross functional team's activities to manage and implement project and/or interrelated projects from requirements submission to the final operational stage. Plans, schedules, monitors and reports on activities related to the projects/programs. Facilitates status review meetings among project team members and/or with senior leadership. Controls project/program requirements, scope and change management execution. Facilitates all communication among cross-functional teams ensuring that all appropriate information is exchanged among key stakeholders. Manage the execution of all assigned projects to accomplish all project/program goals, meet established schedules, and resolve all technical and operational issues.

Minimum Certification Requirements:

Below are the minimum certification requirements for this task area. The Labor category mix (i.e. senior, intermediate, and associate) to meet the certification and performance task requirements shall be identified in proposals as part of the proposed staffing approach.

NOTE: Each labor category proposed for this section shall hold and maintain the following certifications

- Senior Level experience in IT Project Management lifecycle activities, to include:
  - Project management methodologies
  - IT infrastructure
  - IT deployment and operational methodologies
- Project Management certification, shall possess at least one of the following:
  - Project Management Professional PMP
  - Master Project Manager MPM
  - Professional in Project Management

5.7.1 PERFORMANCE TASKS

a. Develop and document project plans.
b. Estimate effort and duration for all tasks required of a project.
c. Establish an overall project timeline with intermediate milestones with associated dates.
d. Develop metrics and measures designed to monitor the progress and success of a project.
e. Identify responsible parties for the execution of all project tasks.
f. Document assigned responsibilities for a project.
g. Identify and document all risks associated with a project.
h. Communicate all risks and associated impacts of a project to all key stakeholders.
i. Coordinate all interrelated activities required of disparate teams and team members.
j. Develop mechanism to communicate ongoing progress of a project.
k. Monitor ongoing progress of the execution of a project.
l. Identify potential obstacles or delays that could adversely affect the progress of a project.
m. Identify mitigation tactics to avoid or overcome potential obstacles or delays to project execution.
n. Communicate potential obstacles or delays to project execution to Government Lead with recommended mitigation strategies.
o. Create and present briefs to senior leadership communicating project status.
p. Create and present briefs to Government Lead gaining the necessary decisions to maintain execution momentum.

5.8 TRANSITION PLAN

General Overview

The Contractor must develop a Transition Plan in the event of contract turnover for the follow-on contract. If the period of performance overlaps with an incumbent Contractor's efforts, the Contractor must collaborate with the incumbent Contractor to facilitate a successful transition-in. The Transition Plan must include the following:

5.8.1 Phase-In Plan

The Contractor must develop and implement a contract transition plan. The full performance start date, which shall be no longer than 90 days after task order award, will begin the contract phase-in period. The phase-in period shall not be shorter than 10 days. During the phase-in period, the Contractor must demonstrate the ability to meet all requirements and ensure all incoming personnel are trained and qualified to perform no later than the full performance start date. The Contractor's personnel must coordinate with Government personnel and the previous contractor's personnel to execute knowledge transfers, provide lessons learned, and ensure continuity of information and documents for the commencement of performance, with no gaps in service after the former Contractor departs.

5.8.2 Phase-Out Plan

The last thirty (30) days in the final Period of Performance of the contract shall constitute the phase-out period. The Contractor must develop and implement a phase-out plan. The phase-out plan must describe how the Contractor intends to coordinate and transfer knowledge to the inbound Contractor, if applicable, and Government personnel and must include the following:

- Program management processes;

- POCs;
- Location of technical and program management documentation;
- Appropriate Contractor-to-Contractor coordination to ensure a seamless transition;
- Schedules and milestones;
- Actions required of the Government;
- Effective communication procedures with the incoming Contractor and Government personnel for the period of the transition via weekly status meetings; and
- Assigned Contractor personnel that will conduct a joint inventory, including condition status assessments, with Government personnel

All facilities, equipment, and materials utilized by the Contractor personnel during performance shall remain accessible to the Contractor personnel during the phase-out period pursuant to the applicable in-processing and out-processing guidelines.

6.0 PERFORMANCE STANDARDS

This is a Performance Based Task Order in accordance with FAR 37.6. The Performance Work Statement provides specific requirements to accomplish the work, documenting the method of approach, analytical tools, and staffing certification requirements. The Government shall monitor the Contractor's performance under this task order using quality assurance procedures developed by the Government known as a Quality Assurance Surveillance Plan. Typical procedures might include random sampling, checklists, inspections, and customer complaints. This is not an all-inclusive list.

7.0 PLACE AND PERIOD OF PERFORMANCE

7.1 Work efforts in support of this task effort will be accomplished at the Marine Corps Support Facility, New Orleans, Louisiana 70114. Contractors are required to work 40 hours/week Monday through Friday, excluding the ten (10) annual U.S. Federal Holidays. Acceptable working hours are between, 0700 – 1800 (Monday – Friday).

In addition to the scheduled U.S. Federal Holidays, Contractor employees shall not report to Marine Corps Support Facility on Mardi Gras Day, which occurs on an annual basis. The Government also anticipates two (2) additional unscheduled administrative holidays on an annual basis for which Contractor employees will not report to Marine Corps Support Facility; these unscheduled administrative holidays may be necessitated by Presidential Executive Orders; facility plumbing/electrical issues; etc.

7.2 The period of performance will be for a one (1) year base period, four (4) one-year option periods, and a six (6) month extension period.

Period	Length	Dates
Base Period	One (1) year	01 July 2020 – 30 June 2021
Option Period One	One (1) year	01 July 2021 – 30 June 2022
Option Period Two	One (1) year	01 July 2022 – 30 June 2023
Option Period Three	One (1) year	01 July 2023 – 30 June 2024
Option Period Four	One (1) year	01 July 2024 – 30 June 2025
6 Month Extension	6 Months	01 July 2025 – 31 Dec 2025

8.0 EQUIPMENT AVAILABLE FOR CONTRACTOR USE.

The government will make available to the contractor, as needed, access to MCEN workstations, electronic access to databases and other information relating to and required for the performance of this PWS.

9.0 TRAVEL

Travel may be required under this task order. The Contractor shall be reimbursed for travel outside the local area in accordance with the terms of travel reimbursement set forth below in Section 10.0. The local area is defined as travel within a 50-mile radius of the Marine Corps Support Facility, New Orleans, Louisiana, 70114.

10.0TRAVEL REIMBURSEMENT

10.1 Contractor Request and Approval of Travel

10.1.1 Any travel under this task order must be specifically requested in writing by the Contractor and approved by the COR, prior to incurring any travel expense. The Contractor shall submit the written request to the COR 14 business days in advance. The travel request shall include as a minimum, the following:

- Contract/task order number
- Date, time, and place of proposed travel
- Purpose of travel and how it relates to the task order
- Contractor's estimated cost of travel with a breakdown of the estimated costs of transportation, lodging, meals, and incidentals; and
- Name(s) of individual(s) traveling.

10.2 The COR will review and approve/disapprove (as appropriate) all travel requests submitted giving written notice of such approval or disapproval to the Contractor.

10.3 Travel Reimbursement. The Contractor shall be reimbursed for the reasonable actual cost of transportation, lodging, meals and incidental expenses. However, actual costs shall be considered reasonable, allowable, and reimbursable only to the extent that they do not exceed on a daily basis the maximum per diem rate in effect at the time of travel as set forth in the DOD Joint Travel Regulations located at https://secureapp2.hqda.pentagon.mil/perdiem/. Actual cost does not include handling charges, general and administrative cost, overhead, profit or any other indirect cost.

10.4 The Contractor shall use the allowable Government personnel rates for transportation and lodging. Reimbursement for airfare shall not exceed the lowest customary standard, coach, or equivalent airfare quoted during normal business hours. The Contractor will not be reimbursed for travel expenses unless audited records for transportation contain evidence, such as original receipts, substantiating actual expenses incurred for travel. In no event will reimbursement exceed the published rates of common carriers. Expenses for lodging, meals and incidental expenses shall be reimbursed to the Contractor, provided that the overnight stay was documented as necessary.

10.5 The task order includes a not-to-exceed funding limitation for travel costs. When the Contractor expects total funding expended for reimbursable travel to reach 85 percent of the total funds available on the travel CLIN, the Contractor shall notify the Contracting Officer and the COR and any other Government official identified by the Contracting Officer. The notice shall state the

estimated amount of additional funds required to continue performance for the period specified in the task order. The Contractor shall not exceed or incur costs that exceed the amount of funding stated on the reimbursable travel CLIN.

10.6 The Government is not obligated to reimburse the Contractor for otherwise reimbursable travel in excess of the funded amount stated on the reimbursable travel CLIN.

10.7 The Contractor is not obligated to incur travel costs in excess of the funded amount stated on the reimbursable travel CLIN unless the Contracting Officer provides the Contractor a funded task order modification to increase the amount of travel CLIN.

10.8 No notice, communication, or representation from any person other than the Contracting Officer shall affect the Government's obligation to reimburse the Contractor.

10.9 Change orders shall not be considered an authorization to exceed the funded amount stated under the reimbursable travel CLIN unless they contain a statement expressly increasing the funded amount of that reimbursable CLIN by a sufficient amount to cover the change order.

11.0 CLOUD COMPUTING AND MODERNIZATION

11.1 Currently Marine Forces Reserve does not have a cloud computing environment. However, there are initiatives both on the local and enterprise level that are exploring that option in the near future. Due to the nature of the IT environment, the Government does not expect the contractor to anticipate the many changes. The potential impacts of cloud computing and modernization on this effort are unknown. Evolution will be addressed with the contractor as it occurs.

12.0 DELIVERABLES

All deliverables are to be submitted to the COR. The Contractor shall provide task order deliverable(s) in a format mutually agreed upon by the Government and the Contractor.

Deliverable	PWS	Details	Due Date
Monthly Status Report/Monthly Briefings	5.1 – 5.7	To include summary of all Individual analysis, exhibits, and reports performed and delivered throughout the month.	Due to the COR no later than the 5th business day following the month of performance.
Individual task area deliverables	5.1 – 5.7	To include individual analysis, exhibits, and reports performed and required throughout each month in various formats (excel, word, access) as required by the COR.	As identified in each task area deliverables section.

Finalized Transition Plan	5.8	Develop and implement a contract transition plan to include a phase in and phase out plan as outlined in section 5.8 of the PWS.	Due 7 business days post award.

13.0 NMCARS 5237.102-90 Inventory of Contracted Services

The contractor shall report contractor labor hours (including subcontractor labor hours) required for performance of services provided under this task order for **Professional IT System Architecture and Application Services task order for Marine Forces Reserve** via a secure data collection site.

The contractor is required to completely fill in all required data fields using the following web address: https://sam.gov/SAM/.

Reporting inputs will be for the labor executed during the period of performance during each Government fiscal year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year. Contractors may direct questions to the help desk, linked at https://sam.gov/SAM/ .

14.0 PERFORMANCE REQUIREMENTS SUMMARY

Performance Requirements Summary

SERVICE	PWS PARAGRAPH NUMBER	STANDARD	ACCEPTABLE QUALITY LEVEL	SURVEILLANCE METHOD	INCENTIVE / PENALTY
Documentation / Deliverables in accordance with applicable directives	4.1	All documentation / deliverables shall be in accordance with applicable Navy and Marine Corps regulations/manuals and any other specified documentation requirements.	Meets all requirements. Problems encountered are minor and resolved in a satisfactory manner.	COR Review for completion and accuracy	CPARS ratings
Staffing Substitution	4.5; 5.1-5.7	Provide personnel substitution in accordance with contractor staffing plan in an efficient manner in order to avoid a gap in service/ lapse of personnel supporting the required task areas. Once a staffing gap is identified, contractor shall notify the	No more than a 4-week gap in support due to a replacement issue	COR tracking	Contractor shall not invoice for the un-supported labor category within a task area CLIN that is un-supported beyond 4 weeks. Reduction will be calculated by dividing the total amount for the applicable un-supported labor category within a

		contracting officer and COR via email.			task area CLIN by 365 days to get a daily rate, and that daily rate will be applied to the number of days of gap in service (beyond 4 weeks) as a deduction on the monthly invoice until personnel substitution is on-board.
Overall management of tasks	5.0	Provide suitable technical and analytical expertise to ensure technical management, coordinate task activities and provide overall expertise for successful completion of each task area.	Meets all requirements. Problems encountered are minor and resolved in a satisfactory manner	Customer input / random sampling / COR review	CPARS ratings
Efficiency & effectiveness of performance	5.0	Perform task order requirements ensuring an unconstrained flow of information to effectively and efficiently complete requirements within the specified cost and schedule.	Meets all requirements. Problems encountered are minor and resolved in a satisfactory manner	Customer input / random sampling / COR review	CPARS ratings
Responsiveness	5.0	Provide services that allow for a rapid response enabling the Marine Corps Comptroller to meet its regulatory requirements and any other financial requests from higher-level authorities within the chain of command.	Meets all requirements. Problems encountered are minor and resolved in a satisfactory manner	Customer input / random sampling / COR review	CPARS ratings
Accuracy of Deliverables required by the Task Order	5.0; 11.0	Reports and Other Deliverables are complete and correct when submitted.	No more than 3 substantive errors in content per Deliverable	COR Review for completion and accuracy	CPARS ratings
Timeliness of Deliverables required by the task order	5.1 – 5-7; 11.0	Deliverables shall be submitted in accordance with the delivery requirements required by the PWS.*	100% of the deliverables / reports are submitted within five days of due date.	COR Tracking	CPARS ratings
Transition Plan	5.8	Develop a Transition Plan in the event of contract turnover for the follow-on contract	Meets all requirements and problems encountered are minor and	COR Tracking	CPARS Rating

			resolved in a satisfactory manner.		
Progress Briefings / Monthly Status Reports	11	Written progress briefings are provided to the COR, on a monthly basis (to detail completion of individual tasks and/or specific project areas as required per the PWS or by the COR).	Briefings shall be provided on time and with less than 3 errors per brief.	COR Review: · Random inspection (site visits, telephone calls) · Customer feedback/surveys · Monthly status reports	CPARS ratings

***Note: Deliverables are not counted as late when, on a case-by-case basis, the COR approves later deliverable submission.**

Task Order attachments (Permanent)

Attachment 1, Department of Defense Contract Security Classification Specification DD Form 254

Attachment 2, Quality Assurance Plan

Attachment 6, Staffing Plan submitted on 4.8.2020 (Previously entitled "Agile Defense – Volume 3 – Attachment 4 – Staffing Plan for PriceCost and SF1449.xlxs")

The following have been deleted:
M67861-20-R-0001_PIT_SAAS Q&A
M67861-20-R-0001_PIT_SAAS Q&A

(End of Summary of Changes)